

Croatian International Relations Review - CIRR
XXIII (80) 2017, 97-129
ISSN 1848-5782
UDC 355.02(497.5)
DOI 10.1515/cirr-2017-0022

CIRR
XXIII (80) - 2017

Development of the Croatian National Security Strategy in the Hybrid Threats Context

Drazen Smiljanic

Abstract¹

The development of the new National Security Strategy (NSS) of the Republic of Croatia, begun in November 2016, takes place in a radically different security environment compared to the first (and current) Croatian NSS published in 2002. This paper aims to provide incentives for potential adaptations to the approach and methodology used in Croatia's NSS development, particularly in relation to hybrid warfare. Assuming that the hybrid adversary tends heavily to exploit the vulnerabilities of the targeted state and society, the paper addresses some of Croatia's widely recognized weaknesses that should be taken into consideration in a threat assessment. As a conclusion, the paper proposes some recommendations, including the concept of societal resilience, related to ways to counter hybrid threats.

KEY WORDS:

national security strategy, hybrid warfare, hybrid threats, Croatia, Russia, vulnerabilities, societal resilience

¹ Disclaimer: the views expressed here are solely those of the author in his private capacity, based on public information, and do not in any way represent the views of the Croatian Ministry of Defence or any other entity of the Croatian government.

Introduction

The first, and current, National Security Strategy (NSS) of the Republic of Croatia was endorsed and published in 2002, as “a conceptual document in which the Croatian Parliament, as the highest political and legislative institution, determines and accepts political views on fundamental national security issues” (Croatian Parliament 2002). Since then, a handful of efforts have been made (MoD Croatia 2010) to develop a new strategy but none of them was finalized with an endorsed document. The latest effort, begun in November 2016, calls for “redefining the concept of national security and the related institutions” and defining a security system that is in line with recent internal and external political and economic changes (HINA 2016).

The need for a redefinition of the concept of national security and related institutions arguably stems from changes in how the very notion of security is perceived in Croatia, as well as from the changed security environment. The period since the end of the Homeland War², and the 2000s in particular, has been marked by relative complacency regarding risks related to direct conventional threats against the Republic of Croatia. To a great extent, membership of NATO, and of the EU to a lesser degree, has represented an important guarantee that Croatian security would also be defended by multinational defence capabilities. Most importantly, the Alliance's capacities have provided, and still provide, a robust deterrent capability. However, NATO's military and technological superiority has been challenged with the outbreak of the Ukraine crisis and the emergence of hybrid threats and concepts, commonly known as hybrid warfare. While in terms of political, military and economic power, NATO's superiority has remained unchanged, the new operating concepts, clearly recognized in Russian foreign policy behaviour since 2014, appeared as an unexpected challenge for several NATO members, especially those on the Eastern flank.

Russian politics towards and against Ukraine, especially since 2014, have shown that disturbances of the vital societal functions and violation of

2 According to the Act on the Rights of Croatian Defenders of the Homeland War and Members of their Families (*Zakon o pravima hrvatskih branitelja iz Domovinskog rata i članova njihovih obitelji*), the Croatian Homeland War lasted from 5 August 1990 until 30 June 1996 (Croatian Parliament 2004).

the infrastructure capability to perform its functions were among the most important instruments of their operating concept. Apparently, the Russian objectives were directed at undermining the country's ability to resist the potential aggressor. The Ukrainian example also demonstrated that malicious acts against the key societal functions and critical infrastructure could become a very powerful tool of the state actor, not only the non-state actors, as was the case before. Damage to the critical infrastructure aimed at deteriorating living conditions may, under favourable conditions, force the attacked country to submit to the aggressor, allowing it to achieve its political goals. The Ukraine crisis revealed that the time for complacency, even for NATO members, is over and that the political and military power of the Alliance is being challenged by behaviour that sneaks under the threshold of activation of collective defence mechanisms (e.g. North Atlantic Treaty Article 5), primarily exploiting state and societal vulnerabilities.

Being a complex phenomenon, hybrid warfare and related concepts represent the types of threat that require a holistic approach in conceptualization, planning, organizing and exercising the response to them. The developers of a national security strategy, in designing their models, should recognize the paradigmatic changes in the security environment and the objects of what should be protected (i.e. secured) and how. We also propose use of the systems approach (systems thinking), which is useful in handling the complexity that Croatia's national security is facing and will face in the coming period. Systems thinking may help in approaching national security holistically, focusing more on reducing one's own vulnerabilities.

While the traditional elements of state power remain relevant, the smaller states, like Croatia, even under the umbrella of NATO or as a member of the EU, have to increase their immunity. We argue that, no matter who the adversary could be, revisionist or rival state(s), state or non-state actors, the most efficient national defence measures should include a reduction of societal vulnerabilities. Societal resilience arguably represents one of the most efficient ways to prevent hybrid threats from being effective. Societal resilience has recently been recognized in many countries (Cederberg and Eronen 2015a), as well in NATO and the EU, as the key factor for mitigating societal vulnerabilities.

Theoretical framework

In the following sections, we analyse the notion of national security and the hybrid warfare concept with related terms. After that, we examine implications of the hybrid threat environment for Croatia's national security. We also address some of Croatia's widely recognized weaknesses that should be taken into consideration in any key security and defence strategy threat assessment. Finally, we propose ways to counter hybrid threats, including an expanded approach to strategic planning and the concept of societal resilience.

The national security

Alan Stolberg (2012: 12) found that different nations have different perspectives on what national security is, which are largely inherent in the respective strategic culture of each nation state. Stolberg explains that "the combination of national interests with strategic culture, and a country's understanding of what its security concerns should be, leads to the identification of what the idea of national security will mean for an individual nation-state member of the international system". Finally, the association of the terms "national" and "security" with the concept of strategy will give the national security most of its relevance.

According to George Kennan³ (1948), as cited in Ikenberry and Slaughter (2006: 14), national security is "the continued ability of the country to pursue the development of its internal life without serious interference, or threat of interference, from foreign powers." This kind of perspective was very influential, particularly among the real politics scholars, until the end of the Cold War period, more precisely until the end of the 1990s. The state and its defence from external threats was amongst the highest priorities (or "ends") of most national security strategies at the time. In general,

3 The definition by George Kennan refers to his Comments on the General Trend of U.S. Foreign Policy, George F. Kennan Papers, Princeton University, dated 20 August 1948.

it may be said that national security strategies substantially represented a “nation’s plan for the coordinated use of all the instruments of state power—non-military as well as military—to pursue objectives that defend and advance its national interest” (Doyle 2007: 624). Arnold Wolfers (1952) makes a distinction between security in an “objective sense”, as the absence of threats, and in a “subjective sense”, as the absence of fear. He argues that security is achieved once both components exist. Some scholars in Croatia argue that the most important aspect of national security is that it represents a precondition for social and economic development (Bilandžić 2015, 2017).

Besides the state security, national security encompasses functions and institutions.⁴ In general, security institutions have to evolve and to be transformed to be able to ensure the state’s function to provide security. In the USA, for instance, the most obvious paradigm change related to the security apparatus after the Cold War happened with the 11 September 2001 terrorist attack and the subsequent anthrax mailings on US soil. These events changed the United States’ calculus of national interests and led to the establishment of the Department of Homeland Security (Newmann 2002). The changed post-Cold War security environment, with new threats and challenges, necessitated an additional focus on internal security, consequently involving the crisis management concept. As the threats became more challenging, the response model started to evolve from the departmental towards the interagency model.

Threats and challenges recognized recently as “hybrid” represent an additional challenge in the approach to national security, expanding it to societal (MoD Finland 2010) and human security.

The hybrid warfare concept

Hybrid threats, hybrid operations, hybrid warfare, ambiguous warfare,

4 The Croatian National Security Strategy 2002 comprises under the term national security of the Republic of Croatia: “(1) a certain (achieved or planned) state of security, (2) a functional area of operations for various security institutions along with all social efforts in the field of achieving security goals and (3) the actual security institutions, linked together within an established relations system” (Croatian Parliament 2002).

non-linear warfare, shadow war or grey-zone wars⁵ are just some of the recently formulated expressions related to the hybrid warfare topic. In the broader literature, the concept of hybrid warfare is often the subject of semantic debate. We will employ the term “hybrid” and the ordinary warfare-related derivative for convenience, to align with the common use of the term. Additionally, without intending to reargue the debate existing in open source literature on an adequate name for this topic, we will consider it as a concept. Namely, as the recently finished NATO STO's (2017: 2) research *SAS-127 Hybrid warfare: a case study*, NATO *implications* suggests, hybrid warfare can be seen as “a concept of operations, or perhaps, an operational concept, rather than a strategy or a theory of warfare.” We also adopt the term “hybrid adversary” for an actor applying the hybrid warfare concept and “hybrid threats” as potential actors and trends that exist in the security environment before the hybrid warfare concept is applied (which is more an act).

We dedicate the following sections to discussing some important questions related to the hybrid warfare concept.

Does the hybrid warfare concept represent a new type of warfare?

Contrary to some claims (Barno 2013, 2014; Cederberg and Eronen 2015b), so-called Russian hybrid warfare does not seem to represent anything new or revolutionary in the history of warfare. Most of the elements, such as the use of “fronts” or proxies, were present in earlier conflicts, even during the Cold War (Mansoor 2012; NATO STO 2017). What has been recognized as new, however, is the use of digital media for information operations at local, regional and even international levels. Janis Berzins (2014: 5), for instance, argues that, from the Russian perspective, “the main battle-space is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare.” This approach intends to create a sense of moral and psychological pressure on enemy's armed forces personnel and civil population. In that context,

5 Antulio Echevarria analyses the Ukraine conflict and concludes that Russia exploited the ambiguity to accomplish its objectives outside the normal scope of what military strategists and campaign planners are legally authorized or professionally trained to address. However, he claims that the grey-zone wars are not wars, per se, “as much as they are the outgrowth of strategies aimed at exploiting the West's legalist view of war and its inherent restraints” (Echevarria 2015: 17).

information may be disseminated by means of television stations, websites/ web portals or social media groups and may even include leafleting to the home address.

Another characteristic that represents novelty is the coordinated use of all instruments of state power at low levels, which also accounts for a general improvement. In the case of Russia, the instruments of state power have been used comprehensively, focusing on different domains, sequentially or at the same time.

What is the role of Russia in relation to the hybrid warfare concept?

Hybrid warfare does not exist as an institutionalized concept in either Russia or the West. We adopt the thesis that hybrid warfare is not a Russian-generated theory of warfare and it is worth mentioning that Russian decision-makers claim that they adapted their capabilities to Western behaviour in international relations (Gerasimov 2013; Bartles 2016).

Even though a discernible pattern of its characteristics exist, the hybrid warfare concept should rather be seen as a set of principles, methods and tools, prioritized and, when possible, integrated, skilfully applied to achieve political objectives without escalating into armed conflict. We argue that our (i.e. Western) struggle to describe the hybrid warfare concept lies in the fact that Russian foreign policy behaviour since 2014 represents a certain strategic surprise to our legal norms and capabilities. This surprise also stems from a complacency in our (i.e. the Euro-Atlantic region) economic and military power which, arguably, has not had the desired deterrent effect.

Therefore, when we talk about the hybrid warfare concept, we must be tolerant and willing to cope with a very fluid, changing and transformative theme. The concept, of course, challenges our judgement and perception and should not be underestimated just because, once emerged, it looks similar to what we have seen before. It is particularly important to approach assessment of the hybrid warfare threat properly in the national security strategy as it has a profound impact on ways (usually the need

for an integrated, whole of the government approach) and means (that also go beyond the purely military but affect armed forces in terms of their agility, responsiveness and level of integration with other instruments of state power).

To properly approach the hybrid warfare concept, it is extremely important to assess a threat actor within that actor's own context. To this end, it is critical that the analysis of hybrid warfare's characteristics in the context of the Russo-Ukraine conflict and Russia's foreign policy behaviour in general is grounded on a deep understanding of the historical context (NATO STO 2017).

Nevertheless, a strategic foresight analysis, which is a part of NSS development, must consider hybrid warfare in a more general perspective. A good example of this is the report by the Center for Strategic and International Studies (Conley et al. 2016) which provides key findings on Russia's influence in Central and Eastern Europe. Their findings may be used as the basic elements to describe Russia's foreign policy behaviour related to the use of hybrid warfare methods.

- "Russia has cultivated an opaque network of patronage across the region that it uses to influence and direct decision-making", a web that "resembles a network flow model", which the authors call an "unvirtuous cycle of the Russian influence".
- "Corruption is the lubricant [...] concentrating on the exploitation of state resources to further Russia's networks of influence".
- The networks constitute the vital element of Russia's doctrine which is primarily a "strategy of influence, not of brute force," aimed at "breaking the internal coherence of the enemy system—and not about its integral annihilation" (Conley et al. 2016: X).

Obviously, the methods described above focus primarily on societal vulnerabilities (e.g. governance, internal conflicts, socially divided society, lack of political consensus on the future of the society, corruption, inefficient law enforcement, lack of natural resources and energy dependency on foreign states, etc.). This aspect seems to be the most important element in distinguishing this type of warfare from the more traditional, where

a territory and a battle (i.e. war fighting) are the main paradigm. The Ukraine crisis therefore brought a new dimension to understanding the hybrid warfare concept: during the crisis, the non-coercive dimension of the concept emerged as preponderant while the hard (kinetic) power (i.e. armed forces) was used primarily as a means of threat.

It has to be emphasized that Russia is not the only actor in contemporary international relations that uses hybrid warfare methods. Similar examples, to a certain extent, may be seen in China's behaviour in the South China Sea or ISIL's ability to mobilize people with a fractured identity. However, Russian foreign policy behaviour comprises most of what the broadest understanding of the hybrid warfare concept contains.

How to define the hybrid warfare concept?

Even though we agree that any attempt to create a strict definition of hybrid warfare may create a risk of not encompassing it comprehensively, doing that is still useful, at least to ensure that the concept is comprehended beyond its purely military or defence dimension.

The NATO STO (2017) Research Specialist Team⁶ (RST) determined that there was little value in looking at the definition of hybrid warfare as part of its work. The RST rather decided that the greatest value would come from focusing on understanding the modalities of Russian and Russian-sponsored activities against Ukraine.

The fact is that the definitions and our understanding of the concept evolve as we reveal its characteristics. Before the Ukraine crisis, hybrid warfare was mostly described as conflict comprising a combination of conventional and asymmetric means of violence. This approach apparently did not go beyond the tactical and operational perspective, let alone include society and its economy, critical infrastructure and other instruments of the state power. Peter R. Mansoor describes hybrid warfare as "conflict involving military forces and irregulars (guerrillas, insurgents and terrorists), which could include both state and non-state actors aimed at achieving a common political goal" (Mansoor 2012: 2). The primary trigger for a

⁶ The RST comprised researchers from nine NATO and partners' nations and the research was conducted in partnership with the Ukraine National Institute for Strategic Studies (NISS).

renewed discussion on the character of this concept was actually Russia's engagement in the Ukraine crisis (Giles et al. 2015).

In 2010, NATO developed the document *Bi-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats*. The document aimed to articulate the parameters of hybrid threats facing NATO and recognize areas that might determine the future capability development in NATO. The intention was also to inform higher-level political authorities and lower-level military commanders of the potential implications within their own domains. The document defines hybrid threats as "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives" (NATO 2010: 2).

The perception of hybrid warfare's definition evolved over time and was mainly understood as being applied by "any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour at the same time and battlespace to obtain their political objectives" (Hoffman 2014).

The EU has developed several policy documents that describe hybrid threats, initially to support its Stratcom and EU Military Staff (MS), and later to provide for the Joint Framework on countering hybrid threats. Some of the definitions are:

"Hybrid warfare can be more easily characterized than defined as a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces. By employing hybrid tactics, the attacker seeks to undermine and destabilize an opponent by applying both coercive and subversive methods" (EEAS 2015: 2).

"Hybrid threats can be characterized as a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological, information),

which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organized hostilities. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity with the intention to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize, recruit and direct proxy actors can be vehicles for hybrid threats" (EC 2016: 4).

Definitions of the hybrid warfare concept related to the Ukraine crisis are not the only ones that exist. One of the most comprehensive descriptions of such warfare in the age of globalization was made by two Chinese senior colonels, Qiao Liang and Wang Xiangsui, in 1999. Their main argument was that warfare in the modern world would no longer be primarily a struggle defined by military means; even more, it may not involve the military at all. Liang and Xiangsui (1999: 7) acknowledged the new principles of war that were no longer about "using armed force to compel the enemy to submit to one's will" but rather were "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests".

The concept labelled as hybrid warfare is therefore neither entirely new nor as old or known as some authors claim. However, many of the existing definitions, especially those articulated before 2014, lack comprehensiveness that goes beyond the military domain (i.e. beyond an attempt to describe it as warfare).

Implications of hybrid threat context for Croatia's national security

Arguably, hybrid warfare methods are a reality and are in use by adversaries in shaping the contemporary security environment. From the NATO members' perspective, they are closely connected to Russian

foreign policy behaviour (NATO 2016).⁷ Consequently, the question worth answering is how does the fact that hybrid warfare is a reality affects Croatia's national security?

Croatia's regional security environment and the role of Russia

Although we are not able to produce a reliable intelligence report related to potential or specific activities of Russia against the Republic of Croatia, some information from open sources may help to create a relatively sound perspective on it.

In an interview with Defense News (Judson 2016), during the Halifax National Security Forum, the Croatian President Mrs Kolinda Grabar Kitarović expressed her views on current threats in Croatia's immediate neighbourhood, explicitly labelling Russian involvement:

"Russia has been very much in hybrid warfare [...] and we see these strong connections between [Republic of Srpska's president Milorad] Dodik and Russia [...] that there would be Russian interference through weapons, through tactics, through intelligence, through information and disinformation campaign."

Apparently, Croatia is not perceived by its highest political levels, at least officially, as a target itself but is rather seen as part of a bigger puzzle in which regional instability may have significant implications for Croatia's national security. We assume that it is reasonable to believe that the main issues in relations between the West and Russia are not only developments in Ukraine but lie in "the international status and socio-political system of Russia" (Kreutz 2015: 67). The Russian President Putin often stresses that his country has no aspirations to global leadership and does not want to follow the Soviet example to represent a kind of "saviour to the world". One

7 NATO's Warsaw Summit communiqué (para. 5) explicitly describes hybrid attacks as one of the security challenges for the Alliance. Furthermore, it recognizes Russia's aggressive actions and its demonstrated willingness to attain political goals by the threat and use of force as "a source of regional instability [that] fundamentally challenge the Alliance, have damaged Euro-Atlantic security, and threaten our long-standing goal of a Europe whole, free, and at peace."

example is his speech at the plenary meeting of the Valdai International Discussion Club in October 2014:

“We do not have any claims to world leadership. The idea that Russia is seeking some sort of exclusivity is false [...] we are simply proceeding from the premise that all participants in international relations should respect each other's interests” (President of Russia 2014).

On the other hand, it is evident that Russia positions itself as a Eurasian power, trying to increase its influence in the regions of North Africa and Middle Asia, and intends to block the enlargement of NATO and EU to its “near abroad”. It is therefore reasonable to expect that Russia's primary interests lie in countries like Belarus, Georgia, Armenia, Azerbaijan and, apparently, Ukraine.

Russia's far reaching agenda of “corralling as many former vassals as possible” (Besemeres 2016: 15) back into its sphere of influence through coercive means has become more evident since Mr Vladimir Putin returned to the presidency in 2012. On the other hand, Russia is aware of its weaknesses in terms of power and capabilities compared to the West and is not expected to deteriorate relations with it to escalate these relations militarily. On the contrary, Russia may and does focus on destabilizing the unity of NATO and the EU.

Although the countries in Eastern, Central and North Europe expressed their concerns and worries about Russian foreign policy behaviour after 2014 more loudly,⁸ the region of South-Eastern Europe and the Western Balkans, in particular, is even more susceptible to Russian influence. Some politicians in that area of Europe openly warned about Russian objectives and the need for NATO to respond more forcefully. One example is the views expressed by the former Bulgarian President Mr. Plevneliev, who demanded that the EU and NATO do more to respond to the Russian “hybrid warfare” approach and to counter the rising threat of Russian aggression (Holmes 2015). Recent events in Macedonia where, according to Janusz Bugajski (2017), the Russian's goal is “not only to diminish prospects for Macedonia's entry into NATO and the EU, but even more

8 The direct result of that is NATO's Readiness Action Plan which, among other things, comprises “assurance measures” for NATO member countries in Central and Eastern Europe (NATO 2017).

menacingly to turn the Balkans into a conflict zone that illustrates Western weakness and intensifies Russia's influence", might be a good example of that influence in place. The case of Macedonia is just an extension of the influence Russia already has in place in Serbia and Republika Srpska (Kirillova 2017).

Current developments in the Western Balkans show a growing trajectory of instability. Unfortunately, the EU has lacked an enlargement strategy for Western Balkan countries since 2007. Nevertheless, the EU is still believed to be a major factor in the regional stability. This is confirmed by Mr Jean Claude Juncker's blunt warning to Donald Trump (Barber 2017) against encouraging countries to copy Brexit, arguing that a break-up of the EU could trigger a war in the Western Balkans.

A more subtle way of influencing political and economic dynamics in the region is the financial domain, where the fragility of banking systems may be used for bargaining via pressures (e.g. threatening to pull large deposits), controlled crisis, etc. As argued by Ivan Krastev (2015), the *Financial Times* journalist, the banking systems in the region are fragile and a controlled crisis in the Balkans would give Russia bargaining chips, and deniability.

A generalized assessment of strengths, weaknesses, opportunities and threats (SWOT analysis) of the Republic of Croatia

One of the conclusions of NATO STO's (2017) activity SAS-127 *Hybrid warfare: a case study, NATO implications* was that it is imperative to understand ourselves, since every weakness and vulnerability may be exploited. The results of the analysis that follows represent a generalized and illustrative assessment of the strengths, weaknesses, opportunities and threats (SWOT analysis) of the Republic of Croatia related to its national security. A particular emphasis in this assessment was given to societal vulnerabilities in Croatia that are usually not taken seriously into

consideration during the development of a threat assessment.

Strengths

- Membership of NATO and EU
- Relatively high level of national cohesion (no ethnic/separatists, extremists or other tensions)
- Capable armed forces and law enforcement system

Weaknesses

- Lack of appropriate interagency (inter-sectorial) cooperation at national level (including crisis management)
- Lack of legal and political means for addressing hybrid warfare
- Armed forces entirely dependent on professionals (reserve forces not adequately maintained for force augmentation in terms of personnel and capability)
- Inadequate and insufficient legal and doctrinal basis to counter hybrid strategies
- Negative demographic trends (ageing, depopulation, emigration of the active working population of Croatia to other, more prosperous EU countries)
- Low national economic performance⁹ resulting in growing social inequalities
- Unsustainable public finances, including excessive dependence of the population on state transfers, which consequently exaggerate government spending (Buric and Stulhofer 2016; Lausic 2017)
- Low effectiveness of the legal system¹⁰
- Political clientelism (crony capitalism) and systemic political corruption (Bilandžić 2015)

9
The Bloomberg prediction "Meet 2016's Worst Economic Performers", puts Croatia in a group of the ten worst performing economies in 2016 (Tartar et al. 2016). The fact that Japan, Finland and Switzerland are in the same group may sound soothing but doesn't change the fact that the Croatian economy is far from being exemplary.

10 Ibid.

- High level of energy import dependency¹¹
- Irrationality of territorial organization and hypertrophy of state institutions and agencies

Opportunities

- Existing national consensus (political parties in the Parliament) about the need to develop a comprehensive government approach to national security
- Besides countries in transition, the Croatian neighbourhood consists of consolidated democracies

Threats (Challenges)

- Clash of geopolitical interests of the outer states in the Western Balkans, with a potential spill-over¹² of conflict over the borders
- Negative security trends in the neighbourhood (potential for violent extremism/radicalism, organized crime, illegal/uncontrolled migrations, possible terrorism)
- Political and societal tensions in the neighbourhood (Serbia, Bosnia and Herzegovina): weak states, unfinished processes of political and economic transition

The above assessment shows that, aside from external conditions (the global and regional security environment), Croatia's internal challenges also give cause for concern. Although NATO membership provides an essential deterrent capability against conventional threats, NATO's Warsaw Summit Declaration states that "the primary responsibility to respond to hybrid threats or attacks rests with the targeted nation" (NATO 2016: para.72). However, the Declaration promises that "NATO is prepared to assist an Ally at any stage of a hybrid campaign". The hybrid threats and attacks apparently do not fit automatically under NATO's collective defence umbrella. This kind of uncertainty has led many small

¹¹ Croatia imports 72 per cent of its energy consumption; most of it (91 per cent) refers to fossil fuels (Matutinovic 2014).

¹² NATO uses this term in describing the strategic military perspectives, including the impact of geopolitical trends on security environment, referring to "Spill over of conflict from neighbouring countries along NATO borders, interstate conflict over access to resources, state-on-state conflict including Article V situations, resource wars, frozen conflict, new spheres of influence" (NATO ACT 2015: 15).

NATO countries, particularly those at the northern and southern “vignette” of the European continent, closer to Russia geographically, to put an additional focus on deterrence measures. The issue is, and it is generally acknowledged, that neither all adversaries nor all types of threat may be deterred by employing traditional deterrence strategies. This is particularly the case with non-state actors (Clarke, Gearson and Shaud 2009: 295–297). Deterrence depends upon psychological effects and must fulfil three criteria: capability, commitment and communication (Lonsdale 2008: 50). Considering Russia as a potential threat, some Scandinavian countries (e.g. Norway, Sweden and Finland), joined by Estonia, started developing the threshold concept, which is conceptualized under the premise of denying the aggressor the ability to achieve its goals swiftly and at low cost (i.e. before NATO’s Article V has been activated). In a multinational alliance context, the threshold is considered the deterrence which the national armed forces in place provide. In this view, the sum of the allied forces provides the deterrence while the national forces provide the threshold. The threshold concept and deterrence arguably deserve an independent study, and are currently the topic of the NATO Science and Technology Organization project SAS-131 *The threshold concept for and by smaller forces*. Besides capable and relevant armed forces, it is very important to identify and assess the vital functions of the society, safeguarding and building resilience in them. Resilience in that case works as a means of dissuading the deterred from aggression, since the costs for the aggressor of creating harm increase with the straightforwardness of security measures used to protect the essentials of the society of the deterrer.

Ways to counter hybrid threats

The organization of a robust national defence to cope with hybrid threats requires a different approach from the current traditional one to deal with more or less conventional and asymmetric threats that comprise an armed attack or/and armed conflict. The instabilities in which hybrid warfare principles are implemented show the inadequacy of the military as a particular instrument of national power able to respond to them.

"In hybrid conflicts, armed forces are not a primary tool to exert military force: they rather serve as a means to create a scenario of intimidation. The idea of war as a struggle between two armies does not apply here. Consequently, military responses exercised by NATO forces are not the first or most appropriate security policy tool" (Major and Mölling 2015: 1).

Military organization as an instrument of the national power should, therefore, be seen more and more as a means that has to be integrated with other instruments of power to respond adequately to challenges stemming from the hybrid warfare concept.

As already described, hybrid warfare may affect various spheres of the life of a state or society. Countering such threats and challenges should be integrated, based on effective interaction among the various state bodies (i.e. ministries, governmental agencies and institutions, security agencies, and armed and law enforcement forces). Even more, "the multi-pronged hybrid threat demands that defence planners engage all parts of society in defensive efforts. Intergovernmental or interagency efforts are not enough any more" (Cederberg and Eronen 2015a: 2).

Prevention of hybrid threats requires a comprehensive understanding of the nature of the conflict in the contemporary international environment, including an awareness of the factors that affect its emergence and escalation, recognition of the stages of its development and conceptualization of potential ways towards conflict resolution. In Croatia, this capacity does not yet exist and is expected to be developed, to a certain degree, with the Homeland Security System Act (MoD Croatia 2016).

We argue that the concept of ways of responding to hybrid threats should comprise, at least, a continuous process of assessment of the vulnerability of national security (including the vulnerability of the vital societal functions):

Design of the processes and systems of the early warning, its setup and maintenance, based on an integrated (i.e. an inter-sectorial, a whole of government) approach.

Sustainability principles and practices in all three aspects

(economic, social and environmental) implemented in the state's key policy and strategic documents to provide societal "immunity".

Societal resilience developed and supported as a higher level of defence to ensure effective and efficient response to hybrid threats, as well as threats and challenges that usually belong to the scope of crisis management.

An integrated model of using/sharing all national capabilities—all available forces and the means to employ them efficiently and rationally.

The recommendations above require careful strategic planning and coordinated efforts on a societal level to be implemented successfully.

Strategic planning in the contemporary security environment

The traditional approach to strategic planning considers an organization through a set of fixed interests (goals, objectives) juxtaposed against a fixed environment (the world or a set of external conditions). This approach then assumes the development of a strategy for attaining the interests subject to the constraints of the fixed environment (Ascher and Overholt 1983: 6). In international politics, strategy is usually perceived as "a comprehensive way to try to pursue political ends, including the threat or actual use of force, in a dialectic of wills" (Heuser 2010: 27). This approach, however, orients the focus of strategy planning exclusively outwards and assumes the use of force as the exclusive means. The changing trends have already been recognized and some new approaches proposed: see, for example, Buzan, Wæver and de Wilde (1998) regarding securitization and the concept of extended sectors of security.

In the complex security environment (Wijkman 2015), neither the environment itself nor the internal state of an organization (a nation) is fixed

and static. More importantly—and this specifically matters in the hybrid threat context—the internal state (the strength, cohesion vs vulnerabilities, etc.) directly relates to the ability to affect the environment, either in shaping it or in countering threats and dealing with disturbances.

As the NATO STO (2017: 20) RST's final report suggests, "it can be argued that when facing a competent hybrid threat actor, once the problem is recognized it is too late." Therefore, it is important to be able to recognize the signs of hostile activities and combine data from many different sources to raise awareness, recognize, pre-empt, mitigate and respond to what may be very subtle activities. Moreover, although not the sole actor in the process, highly capable conventional military forces (including Special Operations Forces) remain a core component of national deterrence in a hybrid threat context.

This approach to strategic planning requires highly competent expertise and a highly developed strategic culture, which is another challenge, as well as an opportunity, for Croatia's national defence. The fact that there is a gap of 15 years (i.e. 2002–2017) between the two national security strategies suggests that an advanced strategic culture, as well as strategy and policy development capacity, has yet to be built.

Systems approach¹³

The more complex our environment is, the more indicators we have to watch to ensure we can have an appropriate answer to disturbances. Indicators link us to the world, since only by reading the right indicators can we cope with our dynamic environment (that is, be situationally aware). Indicators are also helpful in constructing an image of the state of our environment on which we can make a reliable decision to protect and promote what we hold dear.

¹³ In its most basic definition, a systems approach is "a line of thought in the management field which stresses the interactive nature and interdependence of external and internal factors in an organization" (WebFinance Inc. 2017).

Hartmut Bossel (1996) argues that there are two basic sets of indicators needed for the system to cope with the challenges from the environment, determined by:

1. The system itself (the current state of the system).
2. The interests, needs, or objectives of the operator or observer.

Arguably, the majority of national security strategies are focused on the second set (pursuing political ends), while the first (the system itself) is usually considered and analysed only regarding its capacity to achieve the ends described in the second. In fact, the first set should also comprise an assessment of the system itself, through the perspective of addressing vulnerabilities and weaknesses. We therefore propose the systems approach in designing and executing national strategic planning, which should encompass both sets of indicators. The systems approach (systems thinking) may arguably be very useful in handling the complexity facing nations and the world in the coming decades (Arnold and Wade 2015). The systems approach, in this context, enables the integration of ways and means, as well as internal and external environment of a state and society.

The role of society and societal resilience in defending against hybrid threats

In the hybrid threat environment, a society is, at the same time, an object of aggression and a force that counters aggression. As an object of aggression, it may be exposed to powerful informational, psychological, cultural and other aggressor influences. The aggressor can pursue its goals through influences, manipulation of public perception and destructive processes (supporting identity projects of a particular part of the population, inciting separatism and extremism, and/or provoking political and social destabilization) in the country attacked. Besides the cognitive and affective domain, an adversary may well intend to exploit existing socio-economic inequalities that lead to further social disruptions. Corruption of dependencies on the import of commodities and energy-

generating products may also be a source of societal vulnerability. It is therefore critical to identify the causes of the state's weaknesses and to implement policies to improve the situation to decrease negative impacts and develop ways to enhance resistance of such influences in various fields. This contributes to societal resilience against threats and challenges coming from the security environment, particularly against hybrid threats.

In general, as defined by Markus Keck and Patrick Sakdapolrak (2013), societal resilience comprises three capacities: coping, adaptive and transformative. Societal resilience tends to ensure that society can face and quickly recover from any disturbance and crisis.

Most definitions of resilience outline one or more perspectives, but comprise in general reactive recovery (e.g. the cyber-attack) and/or stability after traumatic events (e.g. natural disaster). We chose the description from Zebrowski (2016: 4) as the starting point:

“At its most general level, resilience is understood as the capacity to absorb, withstand and ‘bounce back’ quickly and efficiently from a perturbation. It is considered to be both a natural property and quality which can be improved within a broad array of complex adaptive systems including critical infrastructures, ecosystems, societies and economies through good governance.”

Societal resilience is not only a dynamic and relational concept but also a profoundly political one. It is a focus of the EU and, as stated in its Global Strategy (2016: 23), the resilience deals with “the ability of states and societies to reform, thus withstanding and recovering from internal and external crises”. Moreover, in the same document, building the “state and societal resilience to our East and South” is defined as one of the top five priorities for the EU's external action. Besides references to resilience in the context of resilient societies, states and democracies, the EU Global Strategy (2016) also comprises the resilience of critical infrastructure, networks and services and the resilience of the EU's democracies.

One important aspect of resilience is that it acknowledges uncertainty and complexity as a contemporary condition. However, it emphasizes internal capacities and capabilities as the way to deal with these

problems rather than external intervention (Juncos 2017). Resilience therefore encompasses more actors (e.g. civil preparedness, as is the case in NATO's approach) and a broader spectrum of resources than a traditional, defence-related approach to national security. Some of the threats and challenges that should be taken care of in the societal resilience framework, relevant for Croatia, may be found in the following list adapted from MoD Finland's Security Strategy for Society (2010) and Stoykov (2016):

- Political, economic and military pressure (from an external actor)
- Disturbances in critical government services
- Terrorism, radicalism and other criminality that endangers social order
- Severe disturbances in border security (including uncontrolled people movement)
- Major accidents and extreme natural phenomena
- Serious disturbances in health and welfare of the population
- Disturbances in energy supply
- Disturbances in power supply
- Disruptions in public utilities
- Disruptions in civil transportation systems and transport logistics
- Disturbances in financial and payment systems
- Disruptions in availability of public financing
- Disruptions in availability of food and water resources
- Disturbances in public information and communication systems
- Dealing with mass casualties

The list above comprises some of the most vital functions to society and is focused on contingencies. However, it does not contain all the challenges mentioned in the list of Croatia's vulnerabilities, as some of them belong to cultural (e.g. structural corruption), legal (e.g. effectiveness of the legal

system) or economic (e.g. energy security) aspects. These issues are of particular importance as they may provide an exploitation opportunity for the hybrid adversary.

It is therefore important to define how societal resilience may become a means to counter hybrid threats. Some proposals, adapted from Yanakiev (2016) are given below.

- Dealing with unknown unknowns ("black swans"). This comprises the necessity to anticipate future circumstances, events or effects that are impossible to predict and plan for.
- Development of proactive government-led comprehensive approaches progressively accompanied by whole-of-society strategies aimed at managing risks and building a resilient society.
- Concentration of the resources and capabilities of different stakeholders (primarily the state's instrument of power but also that of the society, the private sector and individual citizens) to counter hybrid threats. This includes improved public-private cooperation on security and development and modernization of civilian and military capabilities.
- Development of innovative legal concepts and frameworks to address hybrid threats adequately.
- Expanding the missions of existing state institutions in the security sector (i.e. new authorities for intelligence and counterintelligence agencies and armed forces, boosting strategic communication) or creating new organizations.

Conclusion and recommendations

A hybrid adversary seeks to exploit the weaknesses of society. It is therefore important to analyse vulnerabilities across all domains that might be exploited by an opponent, including legal, policy, diplomatic, information, military, economic, financial, intelligence, socio-cultural

and law enforcement. Such a gap analysis should also include legal vulnerabilities that could prevent the creation of an appropriate response to hybrid threats. A follow-up step is to reduce (societal) vulnerabilities and to develop joint contingency plans. Besides that, any relevant (grand) strategy should incorporate measures to reduce vulnerabilities that may be exploited by a potential hybrid adversary. The presented approach often requires political (e.g. policy) measures as well as some paradigm changes (e.g. cultural and structural adaptations). Therefore, awareness among decision-makers on the policy/strategic level should be raised that countering this type of threat and challenge requires not only different ways (strategies and concepts) and means (structures and organization), but also different qualities of an organization, be it a company (e.g. related to cyber threats), a community or a state.

Hybrid threat, as a potential, or hybrid warfare, as an act, is a complex phenomenon. It is complex as it results from the convergence and interconnection of different components which together form a more multifaceted and multidimensional threat. Complexity thus makes the traditional approach to strategic planning - which focuses exclusively on organizational interests (e.g. national values and interests) and the environment (e.g. global and regional security environment) - inadequate.

With regard to means to respond to hybrid threats, while the traditional means (conventional armed forces) may still be valid as an instrument for ensuring territorial defence, protection of sovereignty and deterrence, they need to be used in conjunction with other state instruments of power to respond adequately to hybrid threats. Besides the state instruments of power, the resilience of the whole society (e.g. societal immunity) is needed to ensure deterrence against and response to hybrid threats.

This paper analyses hybrid warfare almost exclusively through the Western perspective since the scope of the research was to enlighten the relevance and approaches to the topic for the Croatian national security strategy.

Bibliography

- Arnold, R. D. and Wade, J. P., 2015. A definition of systems thinking: a systems approach. *Procedia Computer Science*, 44(2015): 669–678.
- Ascher, W. and Overholt, W. H., 1983. *Strategic planning and forecasting: political risk and economic opportunity*. 1st ed. New York: John Willey & Sons.
- Barber, L., 2017. Juncker tells Trump to stop 'annoying' praise for Brexit. *Financial Times*, 24 March [online]. Available at: <https://www.ft.com/content/938452b6-1072-11e7-a88c-50ba212dce4d> (Accessed 26 March 2017).
- Barno, D., 2013. Silicon, iron, and shadow: three wars that will define America's future. *Foreign Policy*, 19 March [online]. Available at: <http://foreignpolicy.com/2013/03/19/silicon-iron-and-shadow/> (Accessed 15 September 2016).
- Barno, D., 2014. The shadow wars of the 21st century. *The war on the rocks*, [online]. Available at: <http://warontherocks.com/2014/07/the-shadow-wars-of-the-21st-century/> (Accessed 15 September 2016).
- Bartles, C. K., 2016. Getting Gerasimov right. *Military Review: The Professional Journal of the U.S. Army*, 96(1): 30–37.
- Berzins, J., 2014. *Russia's new generation warfare in Ukraine—implications for Latvian defence policy*. National Defence Academy of Latvia Centre for Security and Strategic Research. Riga, Latvia: National Defence Academy of Latvia.
- Besemeres, J. F., 2016. *A difficult neighbourhood. Essays on Russia and East-Central Europe since World War II*. Acton: The Australian National University Press.
- Bilandžić, M., 2015. *Otvoreno* [TV program] Croatian Radio-Television 1, 16 March, 22:30. Available at: <http://vijesti.hrt.hr/276465/otvoreno-nacionalna-sigurnost-na-ispitu-31> (Accessed 12 January 2017).

- Bilandžić, M., 2017. *Nacionalna sigurnost Hrvatske: od egzistencijalne ugroženosti do izvoznika sigurnosti i faktora međunarodne stabilnosti*. Lecture given by Prof. Bilandžić at the Dominican monastery, Split, Croatia on 18 January 2017.
- Bossel, H., 1996. Deriving indicators of sustainable development. *Environmental Modeling and Assessment*, 1(1996): 193–218.
- Bugajski, J., 2017. Russia's new Macedonia offensive. *Centre for European Policy Analysis*, 10 April [online]. Available at: http://cepa.org/EuropesEdge/Russias_new_Macedonia_offensive (Accessed 12 April 2017).
- Buric, I. and Stulhofer, A., 2016. In search of the egalitarian syndrome: cultural inertia in Croatia? *Financial Theory and Practice*, 40(4): 361–483.
- Buzan, B., Wæver, O. and de Wilde, J., 1998. *Security: a new framework for analysis*. Boulder, CO: Lynne Rienner.
- Cederberg, A. and Eronen, P., 2015a. How can societies be defended against hybrid threats? *Strategic Security Analysis*, 9(1): 1-10.
- Cederberg, A. and Eronen, P., 2015b. Wake up, West! The era of hybrid warfare is upon us. *Geneva Centre for Security Policy*, 31 August [online]. Available at: <http://www.gcsp.ch/News-Knowledge/Global-insight/Wake-up-West!-The-Era-of-Hybrid-Warfare-Is-Upon-Us> (Accessed 19 January 2017).
- Clarke, M., Gearson, J. and Shaud, J. A., 2009. Post-conference briefing note. In: Cain, A. C. ed. *Deterrence in the twenty-first century – proceedings*. [pdf]. Available at: https://media.defense.gov/2017/Apr/05/2001727306/-1/-1/0/B_0118_DETERRANCE_TWENTYFIRST_CENTURY.PDF (Accessed 10 January 2017).
- Conley, H. A., Mina, J., Stefanov, R. and Vladimirov, M., 2016. *The Kremlin playbook: understanding Russian influence in Central and Eastern Europe*. Washington, DC: Center for Strategic and International Studies.
- Croatian Parliament, 2002. Strategy for the Republic of Croatia's national security. *The Official Gazette of the Republic of Croatia* no. 33/2002, [pdf]. Available at: https://www.soa.hr/UserFiles/File/Strategy_

[Republic_of_Croatia.pdf](#) (Accessed 28 December 2016).

- Croatian Parliament, 2004. Zakon o pravima hrvatskih branitelja iz Domovinskog rata i članova njihovih obitelji. *The Official Gazette of the Republic of Croatia* no. 174/2004.
- Doyle, R. B., 2007. The U.S. national security strategy: policy, process, problems. *Public Administration Review*, 4(2007): 624–629.
- EC, 2016. Joint staff working document EU operational protocol for countering hybrid threats “EU Playbook”. *European Commission*, 11034/16.
- Echevarria, A. J., 2015. How should we think about “grey-zone” wars?. *Infinity Journal*, 5(1):16–20.
- EEAS, 2015. *Food-for-thought paper “Countering Hybrid Threats” ST 8887 2015 INIT*. European External Action Service, Council of the European Union, [pdf]. Available at: <http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf> (Accessed 15 September 2016).
- EU Global Strategy (EUGS), 2016. *Shared vision, common action: a stronger Europe, a global strategy for the European Union's foreign and security policy*. [online]. Available at: http://eeas.europa.eu/top_stories/2016/280616_global_strategy_en.htm (Accessed 15 September 2016).
- Gerasimov, V., 2013. Ценность науки в предвидении (The value of science is in the foresight). *Voyenno-Promyshlennyy Kurier (Military-Industrial Courier)*, 26 February [online]. Available at: <http://www.vpk-news.ru/articles/14632> (Accessed 20 February 2017).
- Giles, K., Hanson, P., Lyne, R., Nixey, J., Sherr, J. and Wood, A. eds., 2015. *Chatham House report: the Russian challenge*. London: The Royal Institute of International Affairs.
- Harris, J., 2000. *G-DAE Working Paper No. 00-04: “basic principles of sustainable development”*. Medford, MA: Tufts University Global Development and Environment Institute.
- Heuser, B., 2010. *The evolution of strategy—thinking war from antiquity to the present*. Cambridge: Cambridge University Press.

- HINA, 2016. Croatia starts drafting national security strategy. *EBLnews*, 3 November [online]. Available at: <https://eblnews.com/news/croatia/croatia-starts-drafting-national-security-strategy-42856> (Accessed 20 January 2017).
- Hoffman, F., 2014. On not-so-new warfare: political warfare vs. hybrid threats. *The war on the rocks*, 28 July [online]. Available at: <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/> (Accessed 12 November 2016).
- Holmes, L., 2015. Russia plans a 'hybrid warfare' campaign aimed at destabilising Europe, says Bulgarian President. *Independent*, 14 November [online]. Available at: <http://www.independent.co.uk/news/world/europe/russia-plans-a-hybrid-warfare-campaign-aimed-at-destabalising-europe-says-bulgarian-president-a6734981.html> (Accessed 12 February 2017).
- Ikenberry, G. J. and Slaughter, A., 2006. *Forging a world of liberty under law: U.S. national security in the 21st century*. Princeton, NJ: Princeton University, Woodrow Wilson School of Public and International Affairs.
- Judson, J., 2016. Interview: President of Croatia Kolinda Grabar-Kitarovic. *Defense News*, 29 November [online]. Available at: <http://www.defensenews.com/articles/interview-president-of-croatia-kolinda-grabar-kitarovic> (Accessed 12 April 2017).
- Juncos, A. E., 2017. Resilience as the new EU foreign policy paradigm: a pragmatist turn?. *European Security*, 26(1): 1–18.
- Keck, M. and Sakdapolrak, P., 2013. What is social resilience? Lessons learned and ways forward. *Erdkunde*, 67(1): 5–19.
- Kirillova, K., 2017. Plans for a "Great Serbia" and the Kremlin's hybrid war in the Balkans. *Euromaidan Press*, 24 January [online]. Available at: <http://euromaidanpress.com/2017/01/24/plans-for-a-great-serbia-and-the-kremlins-hybrid-war-in-the-balkans/#arvldata> (Accessed 12 April 2017).
- Krastev, I., 2015. The Balkans are the soft underbelly of Europe. *Financial Times*, 14 January [online]. Available at: <https://www.ft.com/>

content/2287ba66-8489-11e4-bae9-00144feabdc0 (Accessed 3 February 2017).

- Kreutz, A., 2015. *Russia's place in the world*. New York: Algora Publishing.
- Lausic, F., 2017. Dramatično upozorenje: "Ina bi mogla postati recept za novu katastrofu". *Slobodna Dalmacija*, 4 February [online]. Available at: <http://www.slobodnadalmacija.hr/novosti/biznis/clanak/id/466144/dramaticno-upozorenje-ina-bi-mogla-postati-recept-za-novu-katastrofu> (Accessed 12 February 2017).
- Liang, Q. and Xiangsui, W., 1999. *Unrestricted warfare*. Beijing: PLA Literature and Arts Publishing House. Available at: <http://www.cryptome.org/cuw.htm> (Accessed 10 October 2016). Edition in French: Liang, Q. and Xiangsui, W., 1999. *La guerre hors limites*. Paris: Editions Payot & Rivages pour l'édition de poche, l'édition 2006.
- Lonsdale, D. J., 2008. Part I strategy. In: Jordan, D., Kiras, J. D., Lonsdale, D. J., Speller, I., Tuck, C. and Walton, C. D. eds. *Understanding modern warfare*. Cambridge: Cambridge University Press.
- Major, C. and Mölling, C., 2015. A hybrid security policy for Europe: resilience, deterrence, and defence as leitmotifs. *Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs*. SWP Comments No. 22.
- Mansoor, P. R., 2012. Introduction: hybrid warfare in history. In: Murray, W. and Mansoor, P. R. eds. *Hybrid warfare: fighting complex opponents from the ancient world to the present*. New York: Cambridge University Press. pp.1–17.
- Matutinovic, I., 2014. Industrial policy for sustainability. In: Domazet, M. and Marinović, J. D. eds. *Sustainability perspectives from the European semi-periphery*. Zagreb: IDIZ and Heinrich Boll Stiftung. pp. 277–293.
- MoD Croatia, 2010. National Security Strategy draft presented. *Ministry of Defence of the Republic of Croatia*, 23 December [online]. Available at: <https://www.morh.hr/en/news/press-releases/6610-national-security-strategy-draft-presented.html> (Accessed 18 February 2017).
- MoD Croatia, 2016. Commission launches work on drafting national

security documents. *Ministry of Defence of the Republic of Croatia*, 24 November [online]. Available at: <https://www.morh.hr/en/about-us/243-morh/hrvatsko-vojno-uciliste-kategorija/idde/idde-news/13732-commission-launches-work-on-drafting-national-security-documents.html> (Accessed 12 February 2017).

MoD Finland, 2010. Security strategy for society. *Ministry of Defence Finland. Government Resolution 16.12.2010*. [online]. Available at: http://www.defmin.fi/en/publications/strategy_documents/the_security_strategy_for_society (Accessed 7 January 2017).

NATO, 2010. Bi-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats. *NATO SACEUR and SACT*, [pdf]. Available at: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (Accessed 10 January 2017).

NATO, 2016. NATO Warsaw Summit communiqué. Press release on 9th July 2016. *NATO*, [online] (last updated 10.55 AM on 29 March 2017). Available at: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed 30 March 2017).

NATO, 2017. Readiness action plan. *NATO*, [online]. Available at: http://www.nato.int/cps/en/natohq/topics_119353.htm (Accessed 20 February 2017).

NATO ACT, 2015. *Framework for future alliance operations*. Norfolk, VA: NATO Headquarters Supreme Allied Commander Transformation.

NATO STO, 2016. *SAS-121 Hybrid warfare research specialist team on hybrid warfare*. NATO Science and Technology Organization Activity Final Report.

NATO STO, 2017. *SAS-127 Hybrid warfare: a case study, NATO implications*. NATO Science and Technology Organization Activity Report.

Newmann, W., 2002. Reorganizing for national security and homeland security. *Public Administration Review*, 62(Special Issue): 126–137.

President of Russia, 2014. Meeting of the Valdai International Discussion Club. *President of Russia*, 24 October [online]. Available at: <http://en.kremlin.ru/events/president/news/46860> (Accessed 20 March 2017).

- Stolberg, A., 2012. *How nation-states craft national security strategy documents*. Carlisle, PA: U.S. Army War College, Strategic Studies Institute Monograph.
- Stoykov, M., 2016. Expert assessment: national capabilities for protecting societal resilience against hybrid threats. In: *NATO (North Atlantic Treaty Organization), CD&E Annual Conference*. Sofia, Bulgaria, 14-16 November.
- Tartar, A., Saraiva, C. and Li, C., 2016. Meet 2016's worst economic performers. *Bloomberg*, 11 January [online]. Available at: <http://www.bloomberg.com/news/articles/2016-01-11/meet-2016-s-worst-economic-performers-flirting-with-disaster> (Accessed 20 March 2017).
- WebFinance Inc., 2017. *The business dictionary*. [online]. Available at: <http://www.businessdictionary.com> (Accessed 12 January 2017).
- Wijkman, A., 2015. An increasingly complex and vulnerable world. In: EC (European Commission), *Building resilience in a globalised world conference*. Brussels, Belgium, 30 September [online]. Available at: <https://ec.europa.eu/jrc/en/event/conference/building-a-resilient-europe-in-a-globalised-world> (Accessed 20 February 2017).
- Wolfers, A., 1952. "National security" as an ambiguous symbol. *Political Science Quarterly*, 67(4): 147–165.
- Yanakiev, Y., 2016. Conceptualizing the role of societal resilience in countering hybrid warfare. In: *NATO (North Atlantic Treaty Organization), Concept Development and Experimentation Annual Conference*. Sofia, Bulgaria, 14-16 November.
- Zebrowski, C., 2016. *The value of resilience: securing life in the twenty-first century*. New York: Routledge.

Drazen Smiljanic (drazen.smiljanic@morh.hr) is the Head (Director) of the Centre for Defence and Strategic Studies at the Croatian Defence Academy in Zagreb, Croatia. Colonel Smiljanic is an active military officer and a lecturer in Defence Economics at the Croatian Military Academy whose current assignment comprises the responsibility of Croatian national coordinator in NATO's Science and Technology Organization. His research activities are focused on the key aspects of national security and defence (strategic foresight analysis, strategy/concept development, strategic management of the national defence and leadership development). He is currently a PhD student at the University of Defence in the Czech Republic, in the field of defence economics, focusing on sustainability as the driving principle of shaping the modern national security strategy and sustainable defence.